

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Promoting Technological Solutions to Combat)	GN Docket No. 13-111
Contraband Wireless Device Use in Correctional)	
Facilities)	

COMMENTS OF INPIXON

I. INTRODUCTION AND SUMMARY

Inpixon (“Inpixon” or “Company”) hereby respectfully submits its initial comments in response to the *Report & Order and Further Notice of Proposed Rulemaking* (“*FNPRM*”) that the Federal Communications Commission (“FCC” or “Commission”) released on March 24, 2017 in the above-captioned proceeding.

Inpixon combines precise frequency sensing capabilities with a powerful data visualization and analytics platform to provide correctional facilities personnel with real-time intelligence on the form and location of contraband wireless device usage on their premises. The Company provides its customers with comprehensive mobile cyber situational awareness encompassing not just CMRS frequency usage, but also usage of Wi-Fi, Bluetooth, and other communicative frequencies. Moreover, as a fully passive solution, Inpixon technology does not pose a threat of interference to communications in the surrounding community.

Inpixon shares the Commission’s public safety concerns and supports the overall policy objectives of the *FNPRM*. The Company encourages the FCC to support whichever legal process will most efficiently and effectively address the threat posed by identified, unauthorized

wireless devices in correctional facilities. Inpixon also recognizes that contraband wireless activities via the Commercial Mobile Radio Service (“CMRS”) need to be managed and controlled and accordingly sees value in the Commission’s efforts to amend its Part 20 rules. However, tech-savvy inmates can and do utilize Wi-Fi, Bluetooth, and other wireless standards to operate contraband wireless devices. For that reason, Inpixon urges the Commission to pursue technical and regulatory solutions which address the full spectrum of contraband wireless communications – not just CMRS usage.

II. STATEMENT OF INTEREST

Inpixon is a longstanding industry leader in providing Indoor Positioning Analytics (“IPA”) to enable enterprise and government entities to detect, locate, and track wireless devices on their premises. Inpixon works with dozens of customers, public and private, with IPA solutions. For example, in the corrections space, Inpixon has worked with a Canadian correctional institution with a capacity of 600 inmates. During Inpixon’s first year of operations in said facility, staff confiscated approximately 70 phones— half of which were directly attributable to Inpixon’s detection solution. The Company is accustomed to working in security-critical environments and has a robust track record serving federal laboratories, intelligence facilities, and military installations. As a fully passive solution, Inpixon IPA does not pose a threat of interference to neighboring communications.¹

¹ Inpixon’s solution is passive in that it relies on sophisticated “listening” capabilities to detect and locate wireless device usage. Inpixon’s solutions currently do not block or jam any wireless frequencies.

Inpixon aptly describes its services as “GPS for the indoors.” Inpixon IPA consists of two essential components: sensing and analysis. Using patented algorithms, Inpixon’s sensors trilaterate, localize, and monitor all accessible cellular, Wi-Fi, Bluetooth, and other radiofrequency signals. The Company’s encrypted analytics platform immediately displays detected wireless device activity on designated facility maps or floor plans, providing its customers with a comprehensive picture of wireless communications in their facilities.²

Inpixon IPA offers correctional facilities administrators 24/7 situational awareness with crucial real-time alerts and location information on contraband wireless devices. Armed with such information, correctional institutions can either immediately dispatch personnel to confiscate contraband devices, or track the device for investigative purposes to unveil patterns in contraband wireless device usage. Inpixon recognizes that unauthorized communications occur on cellular networks, Wi-Fi, Bluetooth, and other wireless technology standards. Accordingly, the company stands ready to provide correctional administrators with the holistic signals intelligence they require to isolate, investigate, and eradicate unauthorized wireless communications.

III. EFFECTIVE COORDINATION BETWEEN SERVICE PROVIDERS AND CORRECTIONAL FACILITIES IS ESSENTIAL.

Contraband wireless device usage in correctional facilities is a complicated issue best addressed through a coordinated, collaborative process. Inpixon commends the Commission for further investigating avenues to improve the interdiction process, and supports

² A more detailed description of Inpixon’s technology is attached.

rules that will increase and expedite collaboration between pertinent service providers and correctional facilities personnel. The Company supports the general thrust of the *FNPRM*, recognizes the value of a “process for wireless providers to disable contraband wireless devices once they have been identified,”³ and particularly welcomes the Commission’s inquiry into “additional methods and technologies that might prove successful in combating contraband device use in correctional facilities.”⁴

With respect to disabling identified contraband devices, the Commission seeks comment on the respective merits of FCC rule and court order-based approaches to termination.⁵ Inpixon supports whichever process will most effectively and efficiently eliminate the threat posed by the identified contraband wireless devices. Regarding additional methods and technological solutions, the Commission seeks comment on “quiet zones,”⁶ “network based solutions,”⁷ “beacon technology,”⁸ and “any other new technologies designed to combat... contraband wireless devices in correctional facilities... [as well as] what regulatory steps the

³ *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd at 2337 (2017) (“*FNPRM*”).

⁴ *Id.*

⁵ *FNPRM*, at ¶¶ 79-84.

⁶ *Id.*, at ¶¶ 123-27.

⁷ *Id.*, at ¶¶ 128-29.

⁸ *FNPRM*, at ¶¶ 130-31.

Commission could take”⁹ to address this issue. As is explained below, while CMRS termination is an important facet of combating unauthorized wireless device usage, the threat posed by contraband wireless devices in correctional facilities is not limited to CMRS frequencies.

IV. THE COMMISSION SHOULD PURSUE SOLUTIONS WHICH ADDRESS THREATS POSED ACROSS ALL WIRELESS STANDARDS AND ALL CATEGORIES OF CONTRABAND WIRELESS DEVICES.

While wireless technology standards such as Wi-Fi and Bluetooth play an important role in our economy, they also undeniably complicate the jobs of correctional institution employees tasked with carrying out device interdiction procedures. Consider the following two examples. First, as Chairman Pai recognized in a recent speech, “[i]n Maryland ... an inmate being held in the Baltimore City Detention Center on murder charges used a contraband cellphone to order the murder of a witness to his crime.”¹⁰ Similarly, as the Tennessee Department of Correction noted in its comments on the *FNPRM*, last month, a convicted murderer used a contraband wireless device to access Facebook and taunt the widow of the man he killed.¹¹

The two aforementioned incidents have something important in common – they could just as easily be conducted on Wi-Fi as they could on CMRS. A well-recognized contemporary trend in the wireless commercial mobile industry is that carriers and applications

⁹ *Id.*, at ¶¶ 132.

¹⁰ Ajit Pai, Commissioner, FCC, Remarks at Contraband Cellphone Field Hearing, Columbia, SC, at 2 (Apr. 6, 2016) (“Contraband Cell Phone Speech”).

¹¹ *See* Tennessee Department of Correction *FNPRM* Comments at 4.

increasingly offer calling services that rely completely or predominantly on Wi-Fi rather than CMRS for transmission.¹² If a correctional institution were to rely on a Contraband Interdiction System (“CIS”) that only detected CMRS frequencies, the facility staff would risk remaining in the dark about (and not addressing) unauthorized activities carried out via other wireless solutions.

Unfortunately, inmate usage of non-CMRS wireless standards is a definitive fact rather than a merely abstract or theoretical issue. To give but one example, two inmates in an Ohio prison managed to construct a contraband computer which they subsequently connected to the prison’s Wi-Fi network and used to commit identity fraud and theft.¹³ This incident underscores Inpixon’s broader point – to effectively combat contraband wireless device usage in correctional facilities, the Commission must consider the complete range of devices and wireless standards upon which inmates may rely. Inmates sometimes utilize contraband phones, but they also may turn to other contraband wireless devices such as laptops, tablets, or connected IoT devices.

¹² See, e.g., Todd Mersch, *Can Comcast’s Wi-Fi-First Mobile Service Compete with Wireless Rivals?*, WIRELESS WEEK (Jan. 26, 2017), available at <https://www.wirelessweek.com/article/2017/01/can-comcasts-wifi-first-mobile-service-compete-wireless-rivals> (explaining how Comcast’s new MVNO service will rely primarily on Wi-Fi hotspots for call completion and only utilize the Verizon network as a fallback); Ellen Huet, *Google Unveils Its ‘Project Fi’ Wireless Service*, FORBES (April 22, 2015), available at <https://www.forbes.com/sites/ellenhuet/2015/04/22/google-unveils-wireless-service-project-fi/#2742db463168> (discussing Google’s Wi-Fi first MVNO service).

¹³ See Gaby Del Valle, *Inmates Built Secret Computer for Crime*, DAILY BEAST (Apr. 13, 2017), available at <http://www.thedailybeast.com/inmates-built-secret-computer-for-crime>.

These non-CMRS technologies threaten the correctional facility and the public at large just as much as voice or data usage in CMRS frequencies do. Over the past several years, it has become increasingly feasible for inmates to use small, easily concealable Wi-Fi hotspot units or Bluetooth radio devices to facilitate unauthorized communications. By operating in “infrastructure” or “peer-to peer” modes, these hotspots can conceal their service set identifiers (“SSIDs”) and evade detection by cellular jamming systems. Even if the access point is not smuggled into the correctional facility, a co-conspirator on the outside could drop a Wi-Fi or Bluetooth hotspot near the prison wall along with an external battery, completely unbeknownst to prison staff in the absence of a detection and location solution. Armed with a Wi-Fi connection to an Internet access provider, inmates can use any variety of over the top (“OTT”) voice and messaging apps to communicate. Indeed, once on the Internet, a whole world of possibilities is quite literally available to the enterprising inmate. Similarly, Bluetooth technology can be used to connect to other communication devices, to transfer files, to control IoT technologies, and to tether to other devices.

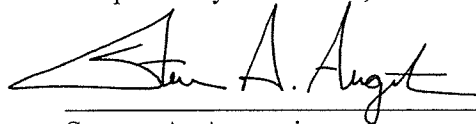
In addressing the role of non-CMRS technologies, the Commission should take into account the evolving capabilities and frequency ranges of such systems. New IoT devices enabling a comprehensive range of communications capabilities come out on a daily basis. Additionally, the effective range of non-CMRS devices continues to increase. Inpixon IPA has detected devices with functional ranges of 35 kilometers using LoRa, while Bluetooth 5 and Wi-Fi have effective ranges of one to three football fields. These expansive capabilities pose new challenges in the effort to secure correctional facilities.

Because inmates do not limit the scope of their illicit activities to CMRS frequencies, the Commission would do well to consider solutions that take advantage of its jurisdiction over Wi-Fi, Bluetooth, and other wireless standards. While modifying Part 20 rules is certainly a worthwhile endeavor, the Commission may also want to consider its options for addressing the threats posed by various Part 15 services.

V. CONCLUSION.

Inpixon looks forward to working with the Commission, correctional facilities, mobile carriers, and other stakeholders in their efforts to interdict and eliminate contraband wireless device usage in correctional institutions. Inpixon applauds the Commission's continued focus on streamlining cooperation between service providers and correctional facilities. The Company also appreciates the Commission's efforts to empower disabling of identified, unauthorized CMRS communications. However, given that inmates make use of readily available alternatives such as Wi-Fi and Bluetooth, Inpixon strongly encourages the Commission to seek solutions that comprehensively address all possible avenues for unauthorized, contraband communications.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Steven A. Augustino", written over a horizontal line.

Steven A. Augustino
Ross G. Slutsky
Kelley Drye & Warren LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007-5108
(202) 342-8612
Counsel to Inpixon

Dated: June 19, 2017